Computing Weierstrass semigroups and the Feng-Rao distance from singular plane models

A. Campillo [*]   J. I. Farrán [*]

July 25, 1999

Abstract

We present an algorithm to compute the Weierstrass semigroup at a point P together with functions for each value in the semigroup, provided P is the only branch at infinity of a singular plane model for the curve. As a byproduct, the method also provides us with a basis for the spaces $\mathcal{L}(mP)$ and the computation of the Feng-Rao distance for the corresponding array of geometric Goppa codes. A general computation of the Feng-Rao distance is also obtained. Everything can be applied to the decoding problem by using the majority scheme of Feng and Rao.

Key words – algebraic curves, singular plane models, approximate roots, Abhyankar-Moh theorem, Weierstrass semigroups, one-point Algebraic Geometry codes, Apéry systems and Feng-Rao distance.

1   Introduction

One of the main problems in the theory of algebraic Geometry codes (AG codes in brief) is the explicit computation of bases for the spaces $\mathcal{L}(G)$, G being a divisor over an algebraic curve. There are some general methods to do this computation, like Coates or Brill-Noether algorithms. In this paper we study an alternative procedure for the particular case $G = mP$, where P is a rational point of the curve, using the structure of the Weierstrass semigroup, the well-known theory of Abhyankar-Moh and the normalization of the curve. This will have also the advantage that it can be used for effective decoding of those codes. Thus, our aim is to review and develop links between coding and singularity theories.

Our method is algorithmic and it assumes to have a singular plane model for the curve with only one branch P at infinity which is defined over the base field. This branch is nothing but the point P in the support of G. A first step uses the Abhyankar-Moh theorem to give a subsemigroup of the Weierstrass semigroup

1

Γ and functions achieving its elements, with the aid of the so-called *algorithm of approximate roots*. A second step computes the rest of the semigroup and corresponding functions by a triangulation algorithm starting from an integral basis for the integral closure of the algebra of the affine part of the curve.

In the case of curves over finite fields, a byproduct of our algorithm can be used for decoding the Algebraic Geometry codes $C(m)$ with divisor of type $G = mP$ by the method of Feng and Rao [10]. This method, based on a majority voting scheme, needs the knowledge of the Weierstrass semigroup at P and functions achieving its values, and it decodes errors up to half the so-called Feng-Rao distance $\delta_{FR}(m)$ (an estimate for the minimum distance which is better than the Goppa distance).

The integer $\delta_{FR}(m)$ can be defined in terms of arithmetical relations among elements in the semigroup Γ. The precise value of $\delta_{FR}(m)$ is known for few classes of semigroups as, for instance, for (many elements of) telescopic semigroups (see [15]). Telescopic semigroups are complete intersection, and so a very special kind of symmetric semigroups (i.e. those such that $c = 2g$, c being the conductor and g the number of gaps). The Abhyankar-Moh semigroup is telescopic, but the Weierstrass semigroup can be quite general.

The last part of the paper is devoted to the computation of the Feng-Rao distance for numerical semigroups S. Our computational method assumes that S is presented by means of its so-called Apéry systems. Such systems are the natural way to describe semigroups when one is dealing with problems involving relations (see [8]). We show a formula (theorem 4.5) to compute $\delta_{FR}(m)$ for a general S. If S is symmetric, this formula is improved (theorem 4.6) for some elements with $m \geq c$. Also for symmetric semigroups, we show how the formula

$$\delta_{FR}(m) = \min\{r \in S \mid r \geq m + 1 - 2g\} \qquad [@]$$

holds for most values $m \in S$ with $c \geq m \geq 2c - 1$ and, moreover, a formula for the minimum element $m_0 \in S$ such that the formula [@] holds for $m > m_0$. An estimate for m_0 was given for telescopic semigroups in [15].

Finally, we show how our algorithmic method to compute Weierstrass semigroups Γ gives also, as a byproduct, an easy way to compute an Apéry system for such semigroups and, hence, the Feng-Rao distance for their elements.

2 Weierstrass semigroups and AG codes

The following section outlines the connection between coding theory and Weierstrass semigroups, and it is abstracted from [14] and [16]. Consider a nonsingular projective algebraic curve χ defined over a finite field $\mathbb{F}$ such that χ is irreducible over $\overline{\mathbb{F}}$. One-point geometric Goppa codes are constructed as follows. Take $n + 1$ different $\mathbb{F}$-rational points $P_1, \ldots, P_n$ and P of the curve χ,

and take a positive integer m. Thus, one can consider the linear map

$$ev_D \; : \; \mathcal{L}(mP) \longrightarrow \mathbb{F}^n$$
$$f \mapsto (f(P_1), \ldots, f(P_n))$$

and define the linear code $C(m)$ as the dual space of $Im\,(ev_D)$, whose length is obviously n. Denote by $k(m)$ and $d(m)$ the dimension over $\mathbb{F}$ and the minimum distance of the linear code $C(m)$ respectively, where the integer $d(m)$ is the minimum value of non-zero entries of a non-zero vector of $C(m)$. Goppa estimates for $k(m)$ and $d(m)$ are derived from the *Riemann-Roch formula* as follows (see [21] for more details). If $2g - 2 < m < n$, then

$$\left\{ \begin{array}{rcl} k(m) & = & n - m + g - 1 \\ d(m) & \geq & m + 2 - 2g \doteq d^*(m) \end{array} \right.$$

where g is the genus of the curve χ and $d^*(m)$ is the so-called Goppa designed minimum distance of $C(m)$. Apart from the excellent asymptotical behaviour of their parameters (see [21], for instance), the main interest of these codes is that they can be decoded efficiently by the majority scheme of Feng and Rao algorithm, which will be briefly described below.

Fix a rational function $f_i \in \mathbb{F}(\chi)$ with only one pole at P of order i for those values of i for which it is possible, i.e. for the non-negative integers in the Weierstrass semigroup $\Gamma = \Gamma_P$ of χ at P. For a received word $\mathbf{y} = \mathbf{c} + \mathbf{e}$, where $\mathbf{c} \in C(m)$, one can consider the unidimensional and bidimensional syndromes given respectively by

$$s_i(\mathbf{y}) \doteq \sum_{k=1}^n e_k\, f_i(P_k) \quad \text{and} \quad s_{i,j}(\mathbf{y}) \doteq \sum_{k=1}^n e_k\, f_i(P_k)\, f_j(P_k)$$

Notice that the set $\{f_i \mid i \leq m, \; i \in \Gamma\}$ is actually a basis for $\mathcal{L}(mP)$ and hence one has

$$C(m) = \{\mathbf{y} \in \mathbb{F}^n \mid s_i(\mathbf{y}) = 0 \; \text{ for } \; i \leq m\}$$

Therefore one can calculate $s_i(\mathbf{y})$ from the received word $\mathbf{y}$ as

$$s_i(\mathbf{y}) = \sum_{k=1}^n y_k\, f_i(P_k)$$

and thus $s_i(\mathbf{y})$ is called *known* for $i \leq m$.

In fact, it is a known fact that if one had enough syndromes $s_{i,j}(\mathbf{y})$ for $i + j > m$ one could know the emitted word $\mathbf{c}$, and all the involved syndromes can be computed by a majority voting (see [10]).

This decoding algorithm corrects up to half the so-called Feng-Rao distance $\delta_{FR}(m)$ of $C(m)$ (see definition 4.1 below). More precisely, the procedure corrects up to $\left\lfloor \dfrac{\delta_{FR}(m') - 1}{2} \right\rfloor$ errors, where $m' = \min\{r \in \Gamma \mid r > m\}$. In particular, one has $d(m) \geq \delta_{FR}(m')$ (see [16] for a direct proof of this inequality).

Notice that $\delta_{FR}(m)$ only depends on the semigroup Γ. On the other hand, it is known that $\delta_{FR}(m) \geq m + 1 - 2g = d^*(m-1)$ for all $m \in \Gamma$, the right hand side term being the Goppa estimate for the minimum distance. Thus, the method gives an improvement of the number of errors that one can correct for one-point AG codes.

In practice, the main problem is computing Γ and the functions f_i achieving the values of the semigroup Γ in order to carry out this decoding algorithm. On the other hand, a second basic problem is calculating the value of $\delta_{FR}(m)$ if one wants to know the number of errors that one can correct. The aim of this paper is to give an approach to the above two problems with certain conditions.

3   Computing Weierstrass semigroups

In this section we show how the Weierstrass semigroups of curves having a singular plane model with only one branch at infinity can be computed at the same time as functions achieving their values. Everything is based on the theory of Abhyankar and Moh about such plane models, and so this section can be regarded as an application of singularity theory to coding theory.

3.1   Semigroups of plane curves with only one branch at infinity

In the sequel, we will assume that $\mathbb{F}$ is any perfect field, since the hypothesis on the finiteness of $\mathbb{F}$ will not be used. Nevertheless, we are always thinking of finite fields, because of the applications in coding theory. Let χ be a non-singular projective algebraic curve defined over $\mathbb{F}$ such that χ is irreducible over $\overline{\mathbb{F}}$. Let Υ be a plane model for χ with only one branch at infinity, i.e. such that there exist a birational morphism

$$\mathrm{n} \;:\; \chi \to \Upsilon \subseteq \mathbb{P}^2$$

and a line $L \subseteq \mathbb{P}^2$ defined over $\mathbb{F}$ such that $L \cap \Upsilon$ consists of only one geometric point P and χ has only one branch at P. Notice that, a fortiori, both P and the branch at P are defined over the underlying field $\mathbb{F}$, since Υ does. Thus there is only one point of χ lying over P, which will be denoted by $\overline{P}$.

Set $\mathcal{C} = \chi \setminus \{\overline{P}\}$ and $\mathcal{Z} = \Upsilon \setminus \{P\}$. One has the two following additive subsemigroups of $\mathbb{N}$:

$$\Gamma_P \doteq \{-v_{\overline{P}}(f) \mid f \in \mathcal{O}_\chi(\mathcal{C})\}$$
$$S_P \doteq \{-v_{\overline{P}}(f) \mid f \in \mathcal{O}_\Upsilon(\mathcal{Z})\}$$

The first one is nothing but the Weierstrass semigroup of χ at $\overline{P}$; this semigroup contains the second one but they are different unless the curve Υ is non-singular in the affine part. Notice that both $\mathbb{N} \setminus \Gamma_P$ and $\mathbb{N} \setminus S_P$ are finite.

In fact $\mathbb{N} \setminus \Gamma_P$ has g elements, g being the genus of χ, which are the Weierstrass gaps. In order to compute the cardinality of $\mathbb{N} \setminus S_P$, we need the following effective version of a standard fact in singularity theory.

Proposition 3.1 *Let $A = \mathcal{O}_\chi(\mathcal{C})$ and $B = \mathcal{O}_\Upsilon(\mathcal{Z})$ be the respective affine coordinate $\mathbb{F}$-algebras of the curves $\mathcal{C}$ and $\mathcal{Z}$; then one has*

$$\sharp(\Gamma_P \setminus S_P) = dim_{\mathbb{F}}(A/B) = \sum_{Q \in \mathcal{Z}} \delta_Q(\mathcal{Z})$$

where Q ranges over all the closed points of $\mathcal{Z}$ and $\delta_Q(\mathcal{Z}) = dim_{\mathbb{F}}(\overline{\mathcal{O}}_{\Upsilon,Q}/\mathcal{O}_{\Upsilon,Q})$, $\overline{\mathcal{O}}_{\Upsilon,Q}$ being the normalization of the ring $\mathcal{O}_{\Upsilon,Q}$.

Proof:

The second equality follows from the fact that

$$A/B = \bigoplus_{Q \in Sing\ \mathcal{Z}} \overline{\mathcal{O}}_{\Upsilon,Q}/\mathcal{O}_{\Upsilon,Q}$$

where $Sing\ \mathcal{Z}$ is the set of (closed) singular points of $\mathcal{Z}$. In order to prove the first equality, we take an $\mathbb{F}$-basis $\{h_1, \ldots, h_s\}$ of A/B, which can be computed with the aid of the *integral basis algorithm* [1] (see [13], [20] and also [9]).

Set $B^i \doteq B + \mathbb{F}h_1 + \ldots + \mathbb{F}h_i$, for $0 \leq i \leq s$. We proceed by induction, so let $0 \leq i < s$ and assume that we have found functions $g_1, \ldots, g_i$ which are linearly independent over $\mathbb{F}$ such that

$$B + \mathbb{F}g_1 + \ldots + \mathbb{F}g_i = B^i$$

and

$$-v_{\overline{P}}(g_j) \notin \Gamma_P^{j-1} \quad \forall j \leq i$$

where $\Gamma_P^j \doteq S_P \cup \{-v_{\overline{P}}(g_1), \ldots, -v_{\overline{P}}(g_j)\} \subseteq \Gamma_P$.

Now look at h_{i+1}. If $-v_{\overline{P}}(h_{i+1}) \notin \Gamma_P^i$, then set $g_{i+1} = h_{i+1}$ and go on.

Otherwise, there exists $f \in B^i$ with $v_{\overline{P}}(h_{i+1}) = v_{\overline{P}}(f)$ and such that

$$-v_{\overline{P}}(h_{i+1} - f) < -v_{\overline{P}}(h_{i+1})$$

Then we repeat the process with $h_{i+1} - f$ replacing to h_{i+1}. Since one has $h_{i+1} \notin B^i$, it follows that in a finite number of steps we will be able to replace h_{i+1} by

$$g_{i+1} \equiv h_{i+1} \ (mod \ B^i)$$

such that

$$-v_{\overline{P}}(g_{i+1}) \notin \Gamma_P^i$$

---

[1] After [13], the *integral basis algorithm* is efficient whenever the ramification of $B|\mathbb{F}$ is not wild. For our purpose, this procedure will be applied in the hypothesis of proposition 3.6, what actually implies that the ramification is tame.

At the end of the procedure s different elements in $\Gamma_P \setminus S_P$ will be added, and hence $\sharp(\Gamma_P \setminus S_P) \geq dim_{\mathbb{F}}(A/B)$. On the other hand, since $A = B^l = B + \mathbb{F}g_1 + \ldots + \mathbb{F}g_s$ one has that any $h \in A$ can be written in a (unique) way as $h = g + \lambda_1 g_1 + \ldots + \lambda_s g_s$ with $g \in B$ and $\lambda_i \in \mathbb{F}$, the values $v_{\overline{P}}(g_i)$ and $v_{\overline{P}}(g)$ being pairwise different. Thus, one has either $-v_{\overline{P}}(h) \in S_P$ or $-v_{\overline{P}}(h) = -v_{\overline{P}}(g_i)$ for a unique i. This proves the equality.

$\square$

Now our aim is as follows: we intend to describe Γ_P by first computing S_P and the associated functions, and secondly by completing the semigroup up to Γ_P with the corresponding functions. According to the above proposition, this last thing can be done by means of the following procedure.

Algorithm 3.2 (Triangulation algorithm)

Input: S_P, $\mathcal{O}_{\Upsilon}(\mathcal{Z})$ and $\{h_1, \ldots, h_s\}$.

- *Initialize $S = S_P$ and $B = \mathcal{O}_{\Upsilon}(\mathcal{Z})$*

- *For $i = 1, \ldots, s$ do*

    - *Set $g_i = h_i$*
    - *While $-v_{\overline{P}}(g_i) \in S$ do*
        * *Find $f \in B$ such that $-v_{\overline{P}}(g_i - f) < -v_{\overline{P}}(g_i)$*
        * *Set $g_i = g_i - f$*
    - *Set $B = B + \mathbb{F}g_i$ and $S = S \cup \{-v_{\overline{P}}(g_i)\}$*

- *Next i*

Output: S and B.

Remark 3.3 *One can substitute the set $S = S \cup \{-v_{\overline{P}}(g_i)\}$ by the semigroup $S = S - v_{\overline{P}}(g_i) \cdot \mathbb{N}$ in the above algorithm, i.e. in each step one can cover more than one gap and also add the corresponding functions (products of existing data functions) to B. It may yield in general a faster algorithm, since one could stop just when l new values are added. This idea can be done effective after the results of the next section by using Apéry systems (see remark 4.15).*

3.2 Approximate roots

The remaining part of the algorithm, that is, the description of the semi-group S_P and the construction of the corresponding functions, is known from the Abhyankar-Moh theorem and the so-called *algorithm of approximate roots*

which, for the sake of completeness, will be restated below. Both were introduced and developed by Abhyankar and Moh in [4]. In particular, it will be shown that this way to compute the Weierstrass semigroup and the functions is effective and, moreover, the arithmetic properties of the involved semigroups will allow us to compute the Feng-Rao distance with the aid of some extra techniques, what will be done in section **4.3**. First we need the notion of approximate root.

Thus, let S be a ring, $G \in S[Y]$ a monic polynomial of degree e and $F \in S[Y]$ a monic polynomial of degree m with $e|m$. If we write $m = ed$, then G is called an approximate d-th root of F if $deg\,(F - G^d) < m - e = e\,(d - 1)$. The key result is that, provided d is a unit in the ring S, then there exists a unique approximate d-th root of F, which will be denoted $app(d, F)$. You can see a constructive proof in [2], where it is shown in particular that the computation of approximate roots is very efficient. From now on, we will work with the coefficient ring $S = \mathbb{F}[X]$.

Let the affine plane model Υ having only one point at infinity be given by the equation

$$F = F(X, Y) = Y^m + a_1(X)\,Y^{m-1} + \ldots + a_m(X)$$

where m is actually the total degree of the polynomial F, and set $n \doteq deg_X F$.

In the sequel, we will assume moreover that

(H)   *char* $\mathbb{F}$ does not divide either $deg\,\Upsilon$ or $e_P(\Upsilon)$

With the above notations, one has $m = deg\,\Upsilon$ and $n = deg\,\Upsilon - e_P(\Upsilon)$, and thus (H) is equivalent to say that $p = char\,\mathbb{F}$ does not divide either m or n.

In this case, we can actually assume that p does not divide $m = deg\,\Upsilon$. In fact, if m is a multiple of p but n is not, we choose k not divisible by p such that $nk > m$, and by doing a change of variables in the form $X' = X + Y^k$, $Y' = Y$ we get a new affine curve which is isomorphic to the original one[2] but whose degree is not divisible by p. This will be assumed in the sequel for simplicity, and thus we will be able to compute any approximate root of F.

By the sake of economy one wants to avoid the computation of parametric equations for the singularity at infinity, and thus computing the semigroup S_P and corresponding functions directly from the equation of the curve. The parametrization would allow us to compute easily $v_{\overline{P}}$-values, but this can be avoided by using resultants and approximate roots, as it is shown below.

In order to state the *algorithm of approximate roots* from [2], we first agree to set

$$deg_X Res_Y(G, H) = -\infty \ \ \text{if} \ \ Res_Y(G, H) = 0$$

for any couple of polynomials $G, H \in \mathbb{F}[X, Y]$, and

$$g\,c\,d\,(\delta_0, \delta_1, \ldots, \delta_i) = g\,c\,d\,(\delta_0, \delta_1, \ldots, \delta_j)$$

---

[2]In particular, S_P does not change.

if $\delta_0, \delta_1, \ldots, \delta_j$ are integers, $j < i$ and $\delta_{j+1} = \delta_{j+2} = \ldots = \delta_i = -\infty$. Thus, the algorithm works as follows with an input F as above (the case when Y divides F being trivial, we assume the contrary).

Algorithm 3.4 (Approximate roots)

- *Set $d_0 = 0$, $F_0 = X$, $\delta_0 = d_1 = m$, $F_1 = Y$ and $\delta_1 = deg_X Res_Y(F, F_1)$*

- *For i from 2 do*

    - *$d_i = g\,c\,d\ (d_{i-1}, \delta_{i-1})$*
    - *If $d_i = d_{i-1}$ then $h = i - 2$ and STOP else*
        * *$F_i = app(d_i, F)$*
        * *$\delta_i = deg_X Res_Y(F, F_i)$*

- *Next i*

Output: h, $(\delta_0, \ldots, \delta_h)$ and $(F_0, \ldots, F_h)$

Since the sequence $\{d_i\}_{i \geq 1}$ obtained in the above algorithm is a decreasing one of positive integers, there exists a unique positive integer h such that $d_1 > \ldots > d_{h+1} = d_{h+2}$, and hence the algorithm stops. The first application of algorithm 3.4 is the following result, proved by Abhyankar in [3], which provides a criterion for a curve with an only (rational) point at infinity to have only one (rational) branch at this point (and to be absolutely irreducible, as a consequence).

Proposition 3.5 (Criterion for having only one branch at infinity)
Let F be the equation of a plane model with an only point at infinity as above, and assume that char $\mathbb{F}$ does not divide $m = deg\, F$. Let h, d_i and δ_i the integers which are computed by the algorithm of approximate roots. Then the curve has an only (rational) branch at infinity if and only if $d_{h+1} = 1$, $\delta_1 d_1 > \delta_2 d_2 > \ldots > \delta_h d_h$ and $n_i \delta_i$ is in the semigroup generated by $\delta_0, \delta_1, \ldots, \delta_{i-1}$ for $1 \leq i \leq h$, where $n_i \doteq d_i/d_{i+1}$ also for $1 \leq i \leq h$.

The second application of the algorithm of approximate roots is just the computation of S_P and the associated functions by means of the Abhyankar-Moh theorem, which provides us with a set of generators for S_P with nice arithmetic properties. The proof is refered to [4] or [17].

Proposition 3.6 (Abhyankar-Moh theorem)
Let Υ be a plane model with an only branch at infinity, and assume that char $\mathbb{F}$ does not divide $deg\, \Upsilon$. Then there exist an integer h and a sequence of integers $\delta_0, \ldots, \delta_h \in S_P$ generating S_P such that $\delta_0 = deg\, \Upsilon$ and

(I) $d_{h+1} = 1$ and $n_i > 1$ for $2 \leq i \leq h$, where $d_i \doteq gcd\,(\delta_0, \ldots, \delta_{i-1})$ for $1 \leq i \leq h+1$ and $n_i \doteq d_i/d_{i+1}$ for $1 \leq i \leq h$.

(II) $n_i \delta_i$ is in the semigroup generated by $\delta_0, \ldots, \delta_{i-1}$ for $1 \leq i \leq h$ [3].

(III) $n_i \delta_i > \delta_{i+1}$ for $1 \leq i \leq h-1$.

Remark 3.7 *Notice that the restriction on the characteristic of* $\mathbb{F}$ *is necessary, since the plane curve over* $\mathbb{F}_2$ *given by the equation*

$$Y^8 + Y = X^2(X^8 + X)$$

has no affine singularity and an only point at infinity whose Weierstrass semigroup is generated by the elements $\{8, 10, 12, 13\}$. *This example gives a negative answer to a question proposed by Pinkham in [17], since the sequences* $\{8, 12, 10, 13\}$ *or* $\{12, 8, 10, 13\}$ *actually satisfy* **(I)**, **(II)** *and* **(III)**, *but* $\delta_0 = 8$ *or* $\delta_0 = 12$, *respectively, is not the degree of the curve. Thus, a general description for* $\Gamma_P = S_P$ *in this way is still an open problem.*

Curiously, this example comes from coding theory (see [11]), and thus the reason why the Abhyankar-Moh theorem fails is that both m *and* $e_P(\Upsilon)$ *are multiple of 2.*

Remark 3.8 *Semigroups as in proposition 3.6, as well as semigroups of values studied in positive characteristic by Angermüller* [4] *in [5] or Campillo in [7], are a particular case of telescopic semigroups, where only the properties* **(II)** *and* $d_{h+1} = 1$ *are required (see [16]). Being telescopic is equivalent to be free in the sense of [5], what means that every* $m \in S_P$ *can be written in a unique (and effective) way in the form*

$$m = \sum_{i=0}^{h} \lambda_i \delta_i \qquad [\star]$$

with $\lambda_0 \geq 0$ *and* $0 \leq \lambda_i < n_i$ *for* $1 \leq i \leq h$ *(see [16]). From property* **(II)** *one has that these semigroups are complete intersection (i.e. those such that the affine curve defined by them is a complete intersection one) and, in particular, they are symmetric (see [12], [16] and section* **4.1** *below for further details).*

The functions which are needed to achieve the pole orders given by the Abhyankar-Moh theorem can actually be assumed to be successive approximate roots of the equation F, and they can be computed by the algorithm of approximate roots. More precisely, one has

$$\delta_i = I_P(F, F_i) = deg_X Res_Y(F, F_i) \quad \text{for } 1 \leq i \leq h$$

---

[3] Notice that $n_1 \delta_1$ is always a multiple of δ_0. Thus the three properties of the Abhyankar-Moh theorem are trivially satisfied if $h \leq 1$ and $d_{h+1} = 1$.

[4] In such semigroups, property **(III)** in proposition 3.6 is substituted by $n_i \delta_i < \delta_{i+1}$.

where $F_i = app(d_i, F)$, $I_P(F, F_i)$ denotes the intersection number at P of the projective completions of the curves given by F and F_i, and where F_i and δ_i are given by the algorithm of approximate roots (see [1]). In particular, one has $-v_{\overline{P}}(F_i) = \delta_i$. Thus, algorithm 3.4 computes at the same time the generators provided by the Abhyankar-Moh theorem and functions achieving such values in an effective way.

Even more, if the algorithm succeeds, i.e. if one arrives to the end with the properties required by proposition 3.5 [5], we are sure that there is one branch at P, and hence the curve is absolutely irreducible. In case of fail, i.e. if such conditions are not satisfied in any of the steps of the algorithm, one can conclude that the plane curve has more than one branch at P.

Remark 3.9 *In case of having a priori a parametrization for the singularity of the unique branch at P, we could use it to compute contact orders instead of using resultants because of the formula $\delta_i = I_P(F, F_i)$. This would give an alternative for the algorithm.*

Example 3.10 *Consider the affine plane curve $Y^8 + Y^2 + X^3 = 0$ defined over $\mathbb{F}_2$, with only one point at infinity $P = (1 : 0 : 0)$. The degree of the curve is multiple of the characteristic, so with the change $X = X + Y^3$, $Y = Y$ one gets the plane model $F(X, Y) = Y^9 + Y^8 + XY^6 + X^2Y^3 + Y^2 + X^3$, and one can apply the algorithm of approximate roots to F:*

$$F_0 = X \,,\; \delta_0 = d_1 = 9 \,,\; F_1 = Y$$

$$\delta_1 = deg_X Res_Y(F, Y) = 3 \,,\; d_2 = g\,c\,d\,(9, 3) = 3$$

$$F_2 = app(3, F) = Y^3 + Y^2 + Y + X + 1$$

$$\delta_2 = deg_X Res_Y(F, F_2) = 8 \,,\; d_3 = g\,c\,d\,(9, 3, 8) = 1$$

*Thus $h = 2$ and $S_P = \langle 9, 3, 8 \rangle$. As a consequence, there is only one branch at infinity since properties (**I**), (**II**) and (**III**) from proposition 3.6 are satisfied.*

On the other hand, with the notations as in proposition 3.1, take a $\mathbb{F}_2$-basis for A/B:

$$h_1 = \frac{Y(1 + Y^6)}{X + Y^3} \quad h_2 = \frac{Y(1 + Y^6)}{(X + Y^3)(Y^2 + Y + 1)}$$

$$h_3 = \frac{X^2 + Y^6}{Y^2 + Y + 1} \quad h_4 = \frac{Y^2(1 + Y^3)(Y^2 + Y + 1)}{X + Y^3}$$

The values of this functions are $-v_P(h_1) = 13 \notin S_P$, $-v_P(h_2) = 7 \notin \Gamma_P^1$, $-v_P(h_3) = 10 \notin \Gamma_P^2$ and $-v_P(h_4) = 13 \in \Gamma_P^3$. Then change h_4 by

$$g_4 = h_4 + h_1 = \frac{Y(1 + Y^3)(Y^2 + Y + 1)}{X + Y^3}$$

---

[5]Notice that the properties given by the Abhyankar-Moh theorem are just the same which are required by the criterion for one branch at infinity.

and now $-v_P(g_4) = 10 \in \Gamma_P^3$. *Thus, one still has to take the function*

$$g_4 = h_4 + h_1 + h_3 = \frac{Y(1 + Y^3)(Y^4 + Y^2 + 1) + (X + Y^3)^3}{(X + Y^3)(Y^2 + Y + 1)}$$

and now $-v_P(g_4) = 4 \notin \Gamma_P^3$. *Hence, the Weierstrass semigroup at P is*

$$\Gamma_P = \{0, 3, \mathbf{4}, 6, \mathbf{7}, 8, 9, \mathbf{10}, 11, 12, \mathbf{13}, 14, \ldots\}$$

3.3 Application to codes

In particular, the above results allow us to compute a basis of the vector space $\mathcal{L}(mP)$, for every $m \in \Gamma_P$, by collecting just one function with an only pole at P of order r, for each $0 \leq r \leq m$ with $r \in \Gamma_P$. This is essential for the construction and decoding of one-point AG codes, and it can be easily done from the above results as follows.

If $r \in S_P$, one gets in an effective way the writing [$\star$] from the remark 3.8 in the form $r = \lambda_0 \delta_0 + \lambda_1 \delta_1 + \ldots + \lambda_h \delta_h$. Thus, if we have functions f_i with $v_P(f_i) = -\delta_i$ (for instance, those which are obtained from the algorithm of approximate roots), then $f_r = f_0^{\lambda_0} \cdot f_1^{\lambda_1} \cdot \ldots \cdot f_h^{\lambda_h}$ has an only pole at P of order r. Otherwise, if $r \in \Gamma_P \setminus S_P$ the function f_r is constructed by algorithm 3.2.

Remark 3.11 *If we fix previously a semigroup with properties as in proposition 3.6, we can try to find a plane curve F with an only branch at infinity achieving this semigroup, even if p divides $gcd\,(\delta_0, \delta_1)$.*

This last procedure is just the inverse of that we have explained in this section, i.e. let the numbers $\delta_0, \delta_1, \ldots, \delta_h$ with the properties as in proposition 3.6 be given, then one can construct in a recurrent way a sequence of polynomials which are called "approximants" of a polynomial F such that $F = 0$ is a curve with a unique branch P at infinity and semigroup S_P generated by $\delta_0, \delta_1, \ldots, \delta_h$ (this is shown by Reguera in [18], where one can check more details). This has the advantage that one can built directly the examples together with functions (the approximants) having the generators of S_P as pole orders.

Remark 3.12 *By using the affine algebra B instead of the normal affine algebra A (with the notations as in section **3.1**), one can construct "improved Algebraic Geometry codes" as in [15]. More precisely, such codes would be the dual of the functional codes given by $\mathrm{Im}\,(ev_D(\mathcal{L}(mP) \cap B))$. They can also be decoded by the Feng and Rao method in the same way. Now one only needs the semigroup S_P instead of Γ_P, so one avoids the triangulation algorithm 3.2. Moreover, by using remark 3.11 one can directly construct curves with only one branch at infinity and functions achieving the values of a semigroup S_P fixed a priori.*

Finally, the results of this section can be summarized as follows.

Theorem 3.13 *Let Υ be an absolutely irreducible projective plane curve of degree m with only one branch P at infinity which is rational over the base field $\mathbb{F}$. Assume the characteristic of $\mathbb{F}$ is either 0 or it does not divide simultaneously m and $m - e_P(\Upsilon)$. Then, by combining algorithms 3.2 and 3.4 one can compute the Weierstrass semigroup Γ_P and functions achieving the pole orders in Γ_P. As a byproduct, one gets a basis of the vector space $\mathcal{L}(rP)$, for every $r \in \Gamma_P$. Moreover, for each semigroup and generators with the properties as in the Abhyankar-Moh theorem, one can generate curves with S_P equal to that semigroup, without restrictions on the characteristic.*

$\square$

In the next section, we will show how to calculate the Feng-Rao distance for Weierstrass semigroups which have been computed with the above method. In fact, we will focus on a general situation in arithmetic semigroups, just taking into account the arithmetic properties of the semigroups in the theory of Abhyankar-Moh and the modifications given by proposition 3.1.

4 Computing the Feng-Rao distance

In this section, we will compute the Feng-Rao distance as a function defined on any arbitrary numerical semigroup, i.e. a subsemigroup of $\mathbb{N}$. Some formulae will stand for the general case, and then we will focus on some concrete types of semigroups, c.g. symmetric, Abhyankar-Moh (or, more generally, telescopic) and Weierstrass semigroups obtained as semigroups at infinity. Notice that such types of semigroups are also interesting in singularity theory.

4.1 Apéry systems and Feng-Rao distance

In the sequel, we consider numerical semigroups, i.e. subsemigroups S of $\mathbb{N}$ such that $\sharp(\mathbb{N} \setminus S) < \infty$ and $0 \in S$. The number $g \doteq \sharp(\mathbb{N} \setminus S)$ is called the *genus* of the semigroup S. Since the genus is finite, there exists a (unique) element $c \in S$ such that $c - 1 \notin S$ and $c + l \in S$ for all $l \in \mathbb{N}$. The number c is called the *conductor* of S, and one has $c \le 2g$. Thus, the "last gap" of S is $l_g \doteq c - 1 \le 2g - 1$, where k is called a gap of S if $k \in \mathbb{N} \setminus S$.

On the other hand, notice that every $m \ge 2g$ is the $(m + 1 - g)$-th element of S, that is ρ_{m+1-g}, according to the notations of [16]. Finally, the semigroup S is called *symmetric* when $r \in S$ if and only if $c - 1 - r \notin S$, for all $r \in \mathbb{Z}$. This is equivalent to say $c = 2g$, that is to say $l_g = 2g - 1$.

Definition 4.1 *For any semigroup $S \subseteq \mathbb{N}$ with $\sharp(\mathbb{N} \setminus S) < \infty$ and $0 \in S$, the Feng-Rao distance of S is defined by the function*

$$\delta_{FR} \; : \; S \longrightarrow \mathbb{N}$$

$$m \mapsto \delta_{FR}(m) \doteq \min\{\nu(r) \mid r \geq m, \ r \in S\}$$

where ν is the function

$$\nu \ : \ S \longrightarrow \mathbb{N}$$

$$r \mapsto \nu(r) \doteq \sharp\{(a,b) \in S^2 \mid a+b = r\}$$

With the above notations, the following result summarizes some known facts about the functions ν and δ_{FR} for an arbitrary semigroup. One can check the details in [15] or [16].

Proposition 4.2

(i) $\delta_{FR}(0) = \nu(0) = 1$, *and* $2 \leq \nu(m), \delta_{FR}(m) \leq m+1$ *if* $m \in S \setminus \{0\}$.

(ii) $\nu(m) = m + 1 - 2g + D(m)$ *for* $m \geq c$ [6], *where*

$$D(m) \doteq \sharp\{(x,y) \mid x,y \ \textit{are gaps of } S \ \textit{and } x+y = m\}$$

(iii) $\nu(m) = m + 1 - 2g$ *for all* $m \in S$ *with* $m \geq 4g - 1$.

(iv) $\delta_{FR}(m) \geq m + 1 - 2g \doteq d^*(m-1)$ *for all* $m \in S$, *and equality holds if moreover* $m \geq 4g - 1$.

In particular, it follows that $\delta_{FR}(m) = \nu(m) = m + 1 - 2g$ for all $m \in S$ such that $D(m) = 0$. On the other hand, since from **(iii)** one has that ν is an increasing function for $m \geq 4g - 1$ at most, the knowledge of the Feng-Rao distance is finitely determined by the values of ν. In fact, for any $m \in S$ one has

$$\delta_{FR}(m) = \min\{\nu(m), \nu(m+1), \dots, \nu(m')\}$$

where m' is the least element in S with $m' \geq m$ and such that $\nu(m') = m' + 1 - 2g$. Thus, elements $m' \in S$ with $D(m') = 0$ are interesting for calculations. Other interesting kind of elements in S are those satisfying the following equality:

$$\delta_{FR}(m) = \min\{r \in S \mid r \geq m + 1 - 2g\} \qquad [@]$$

In practice, such elements exist and have the advantage that the Feng-Rao distance for them is easy to compute.

Our aim is to give some formulae which will allow us to compute the Feng-Rao distance for an arbitrary semigroup by means of an algorithm, provided a suitable set of generators is given. The main tool which will be used was introduced by Apéry in [6] in order to study semigroups of curve singularities, and it is nothing but the Apéry systems of generators and their relations.

---

[6]Notice that one usually assumes that $m > 2g - 2$ in coding theory, and hence $m \geq c$.

Definition 4.3 *Let $S \subseteq \mathbb{N}$ be a semigroup with $\sharp(\mathbb{N} \setminus S) < \infty$ and $0 \in S$; for $e \in S \setminus \{0\}$ define the Apéry set of S related to e by*

$$\{a_0, a_1, \ldots, a_{e-1}\}$$

where $a_i \doteq min\{m \in S \mid m \equiv i \ (mod \ e)\}$ for $0 \leq i \leq e - 1$.

Usually one takes e as the *multiplicity* of S, that is, $e = e_0 \doteq \min(S \setminus \{0\})$, but actually it is not necessary. On the other hand, notice that one could remove $a_0 = 0$ since it does not add any information about the semigroup. In the sequel, the index i will be identified to the corresponding element in $\mathbb{Z}/(e)$. In fact, one has a disjoint union

$$S = \bigcup_{i=0}^{e-1} (a_i + e\mathbb{N})$$

and therefore the set $\{a_1, \ldots, a_{e-1}, e\}$ is a generator system for the semigroup S, called the Apéry (generator) system of S related to e.

Moreover, let $i, j \in \mathbb{Z}/(e) \equiv \mathbb{Z}_e$ and consider $i + j \in \mathbb{Z}_e$; then

$$a_i + a_j = a_{i+j} + \alpha_{i,j} e$$

with $\alpha_{i,j} \geq 0$, by definition of the Apéry set. The numbers $\alpha_{i,j}$ are called *Apéry relations*.

Under these conditions, every $m \in S$ can be written in a unique way as $m = a_i + le$, with $i \in \mathbb{Z}_e$ and $l \geq 0$. Thus, we can associate to m two *Apéry coordinates* $(i, l) \in \mathbb{Z}_e \times \mathbb{N}$.

In order to compute $\nu(m)$, set $m \equiv (i, l)$, $a \equiv (i_1, l_1)$ and $b \equiv (i_2, l_2)$; since

$$m = a + b = a_{i_1+i_2} + (l_1 + l_2 + \alpha_{i_1,i_2}) e$$

then $l_1 + l_2 = l - \alpha_{i_1,i_2}$. Write $i_1 = k$ and $i_2 = i - k$; if $l < \alpha_{k,i-k}$ the equality $m = a + b$ is not possible, and so we are just interested in the case $\alpha_{k,i-k} \leq l$.

Thus, for $0 \leq i \leq e - 1$ and $h \geq 0$ define

$$B_i^{(h)} \doteq \sharp\{\alpha_{k,i-k} \leq h \mid k \in \mathbb{Z}_e\}$$

With these notations, the following result gives us a formula to compute $\nu(m)$.

Proposition 4.4 $\qquad \nu(m) = B_i^{(0)} + B_i^{(1)} + \ldots + B_i^{(l)}$

Proof:

Suppose $\alpha_{k,i-k} = h \leq l$; then it has been considered at the right sum in the sets defining $B_i^{(h)}, B_i^{(h+1)}, \ldots, B_i^{(l)}$, that is $l - h + 1$ times.

On the other hand, the equality $l_1 + l_2 = l - \alpha_{k,i-k}$ holds for $l - h + 1$ possible pairs l_1, l_2, and so the theorem is proved.

$\square$

Now, if we want to have a formula to compute the Feng-Rao distance, the main remark is that $\nu(m)$ is *increasing in l*, because of the previous formula. Then it suffices to calculate a *minimum in the coordinate i*, what gives only a finite number of possibilities. More precisely, one obtains the following result.

Theorem 4.5 *With the above notations, set* $m = a_i + le$. *For each* $j \in \mathbb{Z}_e$, *take* $m_j = a_j + t_je$, *where* t_j *is the minimum integer such that* $t_j \geq max\left\{\dfrac{a_i - a_j}{e} + l, 0\right\}$. *Then one has*

$$\delta_{FR}(m) = min\{\nu(m_j) \mid j \in \mathbb{Z}_e\}$$

Proof:

By using the above remark on the number $\nu(m)$, the formula follows from the fact that m_j is the minimum element of S with first Apéry coordinate equal to j such that $m_j \geq m$.

□

As a conclusion, computing the Feng-Rao distance is easy if we have the Apéry set related to any non-zero element of the semigroup, and the method works in a quite general situation. Next, we will show how the above facts can be done more precise for the case of symmetric semigroups.

4.2 Symmetric semigroups

Now we will compute the value of $\delta_{FR}(m)$ for many elements $m \in S$, S being a symmetric semigroup, and improve the computation in theorem 4.5 for them. The underlying idea is searching for the values $m \in S$ such that either $\delta_{FR}(m) = \nu(m) = d^*(m-1) = m+1-2g$ or the formula [@] is satisfied; this formula will be called "minimum formula" in the sequel. Our results will partially cover lacks in the results given in [16].

First of all, symmetry can be easily expressed in terms of Apéry sets. In fact, let e be any non-zero element of the semigroup S, and consider the Apéry set $\{a_0, a_1, \ldots, a_{e-1}\}$ related to e. For this Apéry set, consider the index $N \in \mathbb{Z}_e$ such that

$$a_N = \max\{a_0, a_1, \ldots, a_{e-1}\}$$

One can easily check that the last gap of S is just $l_g = a_N - e$, i.e. $a_N = c - 1 + e$. Thus, it is easy to check that S is symmetric if an only if

$$a_i + a_{N-i} = a_N \qquad \forall i \in \mathbb{Z}_e$$

In this case, notice that $l_g = 2g - 1$, and thus $a_N = 2g - 1 + e$. By using this fact and the formula of proposition 4.4, one obtains the following result, which provides us with a formula of $\delta_{FR}(m)$ for a certain range of values in S.

15

Theorem 4.6 *Let S be a symmetric semigroup. Then one has*

$$\delta_{FR}(m) = \nu(m) = m - l_g = m + 1 - 2g = e$$

for all $m = 2g - 1 + e$ with $e \in S \setminus \{0\}$.

Proof:

Take an arbitrary non-zero $e \in S$, and let N be the index in $\mathbb{Z}_e$ such that a_N is the maximum Apéry element related to e. We will first prove the formula for all $m \in S$ such that $m \equiv N \ (mod \ e)$, i.e. for $m = a_N + le$, with $l \geq 0$.

By proposition 4.4, one has

$$\nu(m) = B_N^{(0)} + B_N^{(1)} + \ldots + B_N^{(l)}$$

where $B_N^{(h)} = \sharp\{\alpha_{k,N-k} \leq h \mid k \in \mathbb{Z}_e\}$. But because of the equality $a_k + a_{N-k} = a_N$ for all $k \in \mathbb{Z}_e$, one has $\alpha_{k,N-k} = 0$ for all $k \in \mathbb{Z}_e$, and thus $B_N^{(h)} = e$ for all $h \geq 0$. Hence, $\nu(m) = (l+1)\, e = le + (a_N - l_g) = m - l_g$, and the formula is proved for $\nu(m)$. The formula for $\delta_{FR}(m)$ follows immediately from the definition of the Feng-Rao distance and proposition 4.2 **(iv)**.

In particular, for the fixed e the statement holds for $l = 0$, that is, for $m = a_N = l_g + e$. But e is an arbitrary non-zero element in S, and thus the theorem is proved.

$\square$

Theorem 4.6 shows in particular that the minimum formula [@] holds for half of the elements in the interval $[c-1, 2c-2]$. But, in fact, this conclusion of theorem 4.6 is also true for many other elements in this interval. In order to show it, we forget for a moment of Apéry systems, and for $m \in I \doteq [c, 2c-2]$ define two integers n, q given respectively by the equalities

$$m = n + c - 1 \quad , \quad n + q = c - 1$$

Then one has $m = 2c - 2 - q$, and $n \in S$ iff $q \notin S$. Moreover, from proposition 4.2 **(ii)** and the fact that S is symmetric, it follows that

$$\nu(m) = n + \nu(q)$$

where $\nu(q) \doteq 0$ for $q \notin S$. Thus, in particular, if $n \in S$ one recovers $\nu(m) = n$, what gives a different proof of theorem 4.6.

Assume now that $n \notin S$ and let n' be the least integer in S such that $n' > n$. Consider the element q' given by $n' + q' = c - 1$ and let $\delta = \delta(q) = q - q' = n' - n$ be the distance of q (resp. n) to a gap (resp. non-gap) of S. Notice that $\delta(q) \leq e_0 - 1$, e_0 being the multiplicity of S, since the interval $[n, n')$ consists of gaps and there are at most $e_0 - 1$ consecutive gaps in S.

Theorem 4.7 *Let S be a symmetric semigroup and $m \in I = [c, 2c - 2]$. With notations as above, one has*

$$\delta_{FR}(m) = \min\{n + \nu(q), n + 1 + \nu(q - 1), \ldots, n + \delta - 3 + \nu(q - \delta + 3), n'\} =$$
$$= \min\{\nu(m), \nu(m + 1), \ldots, \nu(m + \delta - 3), n'\}$$

In particular, one has $\delta_{FR}(m) \leq n'$.

Proof :

Since $n' \in S$ one has $\nu(c - 1 + n') = n'$; thus, from 4.2 **(iv)** and the definition of the Feng-Rao distance one has

$$\delta_{FR}(m) = \min\{\nu(m), \nu(m + 1), \ldots, \nu(m + \delta) = n'\}$$

But $\nu(m + \delta - 1) = n' - 1 + \nu(q' + 1) \geq n'$, since $q' + 1 \in S$. Moreover, $\nu(m + \delta - 2) = n' - 2 + \nu(q' + 2) \geq n'$, since $q' + 2 \in S \setminus \{0\}$ and therefore $\nu(q' + 2) \geq 2$ (notice that q' can be negative but only in the case $n' = c$, and in this case $q' = -1$). This proves the theorem.

□

Remark 4.8 *According to the above theorem, the Feng-Rao distance can be computed by using the formula given in proposition 4.4 and taking the minimum of only $\delta - 1$ integers. In order to carry out this computation is better, in principle, to use the first equality in the formula of 4.7, since integers with the size of q are smaller than those with the size of m. Next corollary complements the result of theorem 4.6.*

Corollary 4.9 *Let S be a symmetric semigroup and $m \in I$. With notations as above, the minimum formula [@] holds for m if and only if one has*

$$\nu(\overline{q}) \geq \delta(\overline{q})$$

for every $\overline{q}$ in the interval $[q' + 3, q]$.

In particular, this is satisfied for the cases $n \in S$, $\delta = \delta(q) = 1$ or 2, and when $\delta = 3$ but q is not an irreducible element of S (i.e. a non-zero element of S which is not a sum of two non-zero elements of S).

Proof :

It follows from theorems 4.6 and 4.7. Notice that $\nu(q) \geq 3$ if $\delta = 3$ and q is not irreducible.

□

Remark 4.10 *The condition in the above corollary is easy to check, in practice, for many values of m as, for example, those with small values of q.*

However, by using Apéry systems relative to any non-zero element e of S (for instance $e = e_0$) it is always possible to check it. In fact, $\nu(q)$ can be computed from proposition 4.4 and, in order to compute $\delta = \delta(q)$, we can use the following result.

Proposition 4.11 *Assume that $q \in S$, with Apéry coordinates (related to e) given by $q = a_i + le$. Then δ is the least integer such that $q - \delta < a_{i-\delta}$.*

Proof:

On needs to find the value of S such that $(q - \delta, q] \subset S$ and $q - \delta \notin S$. But if $q \equiv i \ (mod \ \ e)$ one has $q - j \equiv i - j \ (mod \ \ e)$ for all $j \in \mathbb{Z}_e$. Thus, the proposition follows from the definition of Apéry elements.

$\square$

Finally, let q_0 be the smallest integer in S such that $\nu(q_0) < \delta(q_0)$, and set $q_0 = c - 1$ if such an integer does not exist. From corollary 4.9 one has $q_0 \geq e_0 + 2$ and $q_0 = e_0 + 2$ if and only if $e_0, e_0 + 1, e_0 + 2 \in S$ and $e_0 > 2$. This happens, for instance, for the symmetric semigroup whose gaps are $1, 2, \ldots, g - 1, 2g - 1$, with $g \geq 3$. For a general symmetric semigroup, the value of q_0 is, in practice, much bigger.

Now, from proposition 4.2 **(iv)**, the minimum formula holds in the interval $[4g - 1, \infty)$. In fact, from the above results one deduces the whole interval where this formula is satisfied.

Corollary 4.12 *For a symmetric semigroup S, the minimum formula [@] is satisfied in the interval (m_0, ∞), where $m_0 = 4g - 2 - q_0$, but it does not hold for m_0 .*

Proof:

It follows from theorem 4.7, corollary 4.9 and the definition of q_0 .

$\square$

Remark 4.13 *Notice that $m_0 \geq 4g - e_0 - 3$, what gives an estimate for m_0 .*

Example 4.14

- *For the semigroup $S = \langle 9, 12, 15, 17, 20, 23, 25, 28 \rangle$ one has $c = 32$ and $q_0 = 25$, thus [@] is satisfied for $m \geq 38$.*

- *For the semigroup $S = \langle 6, 8, 10, 17, 19 \rangle$ one has $c = 22$ and $q_0 = 19$, thus [@] is satisfied for $m \geq 24$.*

- *For the semigroup $S = \langle 8, 10, 12, 13 \rangle$ one has $c = 28$ and $q_0 = 25$, thus [@] is satisfied for $m \geq 31$.*

- *For the semigroup $S = \langle 6, 10, 15 \rangle$ one has $c = 30$ and $q_0 = 29$, thus [@] is satisfied for $m \geq 30$.*

4.3 Semigroups at infinity

In the situation of semigroups at infinity being computed as in section **3**, we want to calculate the Apéry set of the semigroup S_P related to $e = \delta_0 = deg\, \Upsilon$, with the assumptions of the Abhyankar-Moh theorem. In general, we can solve this problem for an arbitrary telescopic semigroup S.

Recall that, for such a semigroup, the main fact is that any $m \in S$ can be written in a unique way in the form

$$m = \sum_{k=0}^{h} \lambda_k \delta_k = \lambda_0 \delta_0 + \sum_{k=1}^{h} \lambda_k \delta_k$$

with $\lambda_0 \geq 0$ and $0 \leq \lambda_k < n_k = d_k/d_{k+1}$ for $1 \leq k \leq h$. But this means exactly that the possible *Apéry elements* related to δ_0 are only those with $\lambda_0 = 0$. On the other hand, the number of all the possible elements of this form is

$$n_1 n_2 \ldots n_h = \delta_0$$

since $d_1 = \delta_0$ and $d_{h+1} = 1$. Thus, all of them are different modulo δ_0 and minimum with this property, and hence they are just the elements of the Apéry set of S related to δ_0.

As a consequence, for a given $m \in S$ written in the form

$$m = \lambda_0 \delta_0 + \sum_{k=1}^{h} \lambda_k \delta_k$$

we can compute its *Apéry coordinates* $l = \lambda_0$ and $i \in \mathbb{Z}/(\delta_0)$ such that $i \equiv \sum_{k=1}^{h} \lambda_k \delta_k \pmod{\delta_0}$. Thus, we can easily compute a_i and $\alpha_{i,j}$, and so $\nu(m)$ and $\delta_{FR}(m)$ for a telescopic semigroup and, in particular, for a semigroup at infinity S_P when computed by the algorithm of approximate roots, under the assumptions of the Abhyankar-Moh theorem.

In fact, the values of $\delta_{FR}(m)$ are known for many values of $m \in S$, if S is telescopic. More precisely, apart from the results given by proposition 4.2, if we assume moreover that $\delta_h = \max\{\delta_0, \delta_1, \ldots, \delta_h\}$, then the minimum formula [@] is true for every $m \in [c, 2c-2]$ in the interval [7] $[(4g-1)-(d_h-1)\delta_h, 4g-1)$, i.e. one has $q_0 \geq (d_h-1)\delta_h$. Also one has $\delta_{FR}(m) = j+1$ if $(j-1)\delta_h < m \leq j\,\delta_h \leq (d_h-1)\delta_h$ (see [16]). Hence, the Feng-Rao distance is unknown in general for the interval $[(d_h-1)\delta_h + 1, (4g-2)-(d_h-1)\delta_h]$, but nevertheless it can be

---

[7]This result is improved by corollary 4.12. For example, the telescopic semigroup $S = \langle 8, 10, 12, 13 \rangle$ the formula [@] is satisfied from $m = 31$ instead of $m = 42$, and for the telescopic semigroup $S = \langle 6, 10, 15 \rangle$ the formula [@] is satisfied from $m = 30$ instead of $m = 44$.

computed by the formulae of proposition 4.4 and theorem 4.5. Notice that, for example, one has

$$\nu\left(\sum_{k=1}^{h}\lambda_k\delta_k\right) = (\lambda_1 - 1)(\lambda_2 - 1)\dots(\lambda_h - 1)$$

for the Apéry elements.

Now, we want to compute the Apéry set related to $e = deg\,\Upsilon$ for the Weierstrass semigroup $\Gamma_P = S_P + b_1\mathbb{N} + \dots + b_s\mathbb{N}$, where S_P has been computed by means of the Abhyankar-Moh theorem, $s = dim_{\mathbb{F}}(A/B)$ and b_i has been computed as in proposition 3.1. In order to do it, it suffices to solve the following question:

> For a given numerical semigroup S with Apéry set $\{a_0, a_1, \dots, a_{e-1}\}$ related to $e \in S \setminus \{0\}$, computing the Apéry set $\{\overline{a_0}, \overline{a_1}, \dots, \overline{a_{e-1}}\}$ for the semigroup $\overline{S} = S + b\mathbb{N}$ related to $e \in \overline{S} \setminus \{0\}$.

In fact, after having solved the above question, by repeating the procedure a finite number of steps one gets the Weierstrass semigroup Γ_P with its Apéry basis (see remark 3.3).

First, for a given b one wants to know wether b is already in S or not, because if it is so, then $S = S + b\mathbb{N}$ and nothing changes. This can be easily tested with aid of the given Apéry set of S as follows:

(i) Calculate $i \in \mathbb{Z}_e$ such that $i \equiv b \,(mod\ e)$.

(ii) Then, $b \in S$ if and only if $l = \dfrac{b - a_i}{e} \geq 0$.

On the other hand, the candidates to be the elements of the new Apéry set are obviously the numbers $m_{j,\lambda} = a_j + \lambda\,b$ with $0 \leq j \leq e-1$ and $0 \leq \lambda \leq e-1$, i.e. the number of possibilities is small. Thus, we proceed as follows:

1. Initialize $\overline{a_i} = a_i$ for $1 \leq i \leq e - 1$ (obviously $\overline{a_0} = a_0 = 0$).

2. Take one of the elements $m_{j,\lambda}$ and compute its remainder i modulo e.

3. Compare $m_{j,\lambda}$ with the value of $\overline{a_i}$; if $\overline{a_i}$ is greater we have to change its value, set $\overline{a_i} = m_{j,\lambda}$ and so on with the next $m_{j,\lambda}$.

At the end of this procedure we get the Apéry set for $\overline{S}$, and the new Apéry relations can be easily computed from them.

Remark 4.15 *The results of this section suggest to present the elements m in a semigroup S as couples $(i, l) \in \mathbb{Z}_e \times \mathbb{N}$ if $m = a_i + l\,e$. Thus, S is given by nothing but the data $\{e \; ; \; a_i$ for $0 \leq i \leq e - 1\}$ with the restrictions $\alpha_{i,j} \geq 0$. In particular, the computations made in section **3.3** to find a function for every*

21

element in the Weierstrass semigroup are easier if we use the Apéry description of the semigroup and functions for each element of the Apéry set.

More precisely, one just saves the data $\{a_0 = 0, a_1, \ldots, a_{e-1}, e\}$ together with the associated functions $\{h_0 = 1, h_1, \ldots, h_{e-1}, h_e\}$ satisfying $-v_P(h_i) = a_i$ for $0 \le i \le e - 1$, and $-v_P(h_e) = e$. Thus, for any $m \in S$ we compute its coordinates (i, l) and then $f_m = h_i \cdot h_e^l$ is the function associated to m. We save in general many generators, but the description of an element $m \in S$ in terms of them is quite fast (just doing a sum and two divisions by e). However, if we save the sequence of non-gaps $\{\rho_i\}$ with the associated functions $\{f_i\}$ we may use much more space, since the ratio g/e can be as large as we want.

On the other hand, the new elements added in the steps of the algorithm 3.2 modify the semigroup changing those data. Thus, such changes can be included in this algorithm, and so the semigroup Γ_P, the functions and the Feng-Rao distance can be computed simultaneously. In particular, this gives an effective answer to the idea which was proposed in remark 3.3.

Finally, for the computation of the Feng-Rao distance we should take into account that in case of Γ_P being symmetric[8], then the calculations can be simplified by means of theorem 4.7 or its corollaries.

References

[1] S. S. Abhyankar, *Lectures on expansion techniques in Algebraic Geometry*, Tata Institute of Fundamental Research, Bombay (1977).

[2] S. S. Abhyankar, *On the semigroup of a meromorphic curve*, Intl. Symp. on Algebraic Geometry, pp. 249-414, Kyoto (1977).

[3] S. S. Abhyankar, *Irreducibility criterion for germs of analytic functions of two complex variables*, Advances in Mathematics **74**, pp. 190-257 (1989).

[4] S. S. Abhyankar and T. T. Moh, *Newton-Puiseux expansion and generalised Tschirnhausen transformation*, J. Reine Math. **260**, pp. 47-83 and **261**, pp. 29-54 (1973).

[5] G. Angermüller, *Die Wertehalbgruppe einer ebenen irreduziblen algebroiden Kurve*, Math. Zeit. **153**, pp. 267-282 (1977).

[6] R. Apéry, *Sur les branches superlinéaires des courbes algébriques*, C.R. Acad. Sciences Paris **222**, pp. 1198-1200 (1946).

[7] A. Campillo, *Algebroid curves in positive characteristic*, Lecture Notes in Math., vol. 813, Springer-Verlag (1980).

---

[8] With the notations of section **3.1**, this is equivalent to $\mathcal{C}$ being an affine complete intersection curve, as you can see in [19].

[8] A. Campillo and P. Giménez, *Syzygies of affine toric varieties*, to appear in J. of Algebra.

[9] J. I. Farrán, *Construcción y decodificación de códigos álgebro-geométricos a partir de curvas planas: algoritmos y aplicaciones*, Ph.D. thesis, Univ. Valladolid (1997).

[10] G. L. Feng and T. R. N. Rao, *Decoding algebraic-geometric codes up to the designed minimum distance*, IEEE Trans. Inform. Theory **39**, pp. 37-45 (1993).

[11] J. P. Hansen and H. Stichtenoth, *Group codes on certain algebraic curves with many rational points*, AAECC, vol. 1, pp. 67-77 (1990).

[12] J. Herzog und E. Kunz, *Die Wertehalbgruppe eines lokalen Rings der Dimension 1*, Sitz. Ber. Heidelberger Akad. der Wissenschaft 2, Abhandlung (1971).

[13] M. van Hoeij, *An algorithm for computing an integral basis in an algebraic function field*, Maple V Release 4 share library, preprint (1996).

[14] T. Høholdt and R. Pellikaan, *On the decoding of algebraic-geometric codes*, IEEE Trans. Inform. Theory **41**, pp. 1589-1614 (1995).

[15] T. Høholdt, J. H. van Lint and R. Pellikaan, *Algebraic Geometry codes*, to appear in *Handbook of Coding Theory* (V.S. Pless, W.C. Huffman and R.A. Brualdi Eds., Elsevier).

[16] C. Kirfel and R. Pellikaan, *The minimum distance of codes in an array coming from telescopic semigroups*, IEEE Trans. Inform. Theory **41**, pp. 1720-1732 (1995).

[17] H. Pinkham, *Séminaire sur les singularités des surfaces (Demazure-Pinkham-Teissier)*, cours donné au Centre de Math. de l'École Polytechnique (1977-1978).

[18] A. J. Reguera, *Semigroups and clusters at infinity*, Progress in Mathematics, vol. 134, pp. 339-374, Birkhäuser (1996).

[19] A. Sathaye, *On planar curves*, Amer. J. Math. **99**, pp. 1105-1135 (1977).

[20] B. M. Trager, *Integration of algebraic functions*, Ph.D. thesis, Dept. of EECS, Massachusetts Institute of Technology (1984).

[21] M. A. Tsfasman and S. G. Vlăduţ, *Algebraic-geometric codes*, Math. and its Appl., vol. 58, Kluwer Academic Pub., Amsterdam (1991).